Appendix 1

EAST CAMBRIDGESHIRE
DISTRICT COUNCIL

Internal Audit Progress and Performance Update

October 2023

Introduction

1.1 The Internal Audit service for East Cambridgeshire District Council provides 210 days to deliver the 2023/24 Annual Audit Plan.

1.2 The Public Sector Internal Audit Standards (the Standards) require the Audit Committee to satisfy itself that it is receiving appropriate assurance about the controls put in place by management to address identified risks to the Council. This report aims to provide the Committee with details on progress made in delivering planned work, the key findings of audit assignments completed since the last Committee meeting and an overview of the performance of the audit team.

Performance

2.1 **Delivery of the 2023/24 Audit Plan**

At the time of reporting, fieldwork is either complete or underway in relation to approximately 53% of the planned work.

Progress on individual assignments is shown in Table 1.

2.2 **Are clients satisfied with the quality of the Internal Audit assignments?**

To date, four survey responses have been received in relation to feedback on completed assignments for the 2023/24 audit plan – this is summarised in Table 4.

2.3 **Based upon recent Internal Audit work, are there any emerging issues that impact upon the Internal Audit opinion of the Council's Control Framework?**

Since the last Audit Committee meeting, the Internal Audit team has finalised three audit reports. The key findings were as follows:

Payment Card Industry Data Security Standard (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is a global standard, administered by the PCI Security Standards Council (SSC), which was founded by five major card providers and provides technical and operational requirements to protect cardholder data and sensitive authentication data.

The PCI Security Standards Council is responsible for managing the security standards, whilst compliance is enforced by the major card providers. Every organisation that stores, processes, or transmits card holder data must comply with PCI DSS, regardless of industry or size. Non-compliance with PCI DSS can result in suspension of the ability to accept and process card payments, increased transaction fees, non-compliance fees and/or costs to cover any forensic investigation if there is a breach. This audit reviewed the controls in place to provide assurance over the Council's compliance with the PCI DSS in handling of card payments. The Council received over 34,000 card payments either via telephone, through the Council's customer services department or online forms in 2022/23.

A cloud-based, online payment solution for processing card payments is used by the Council, via a third-party provider, Civica. The Council also has a partnership with Anglian Revenues Partnership (ARP) who process transactions delivering the Revenues and Benefits Services for several local authorities. The audit has confirmed that both the Council and Civica had completed and submitted an annual self-assessment questionnaire and quarterly network scans are carried out. The Council does not, however, obtain its own assurances that third parties handling cardholder data are PCI DSS compliant nor monitor their on-going compliance.

The self-assessment process to date has been led by the Finance team but the Council does not have a nominated PCI DSS compliance lead to oversee the implementation and maintenance of the PCI DSS requirements within the Council's (and third party) systems and processes, and roles, responsibilities and compliance activities for doing so are not formally agreed and documented.

Employees who process card payments are informed of the need to keep card data safe and secure, but it is important for the Council to establish a formal awareness programme to educate employees about the importance of protecting cardholder and the specific requirements outlined in the PCI DSS.

Internal Audit established that there is robust process in place for reporting and dealing with any data breaches and the Council has a clear Information Security Policy and Data Protection Guidance.

Based on the work performed during the audit, assurance opinions were given as follows:

Assurance Opinion		
Control Environment	**Limited**	●
Compliance	**Moderate**	●
Organisational Impact	**Medium**	●

Use of agency staff and consultants

The objective of the audit was to review the accuracy and clarity in the Council's approach to the use of agency workers and consultants. The audit seeks to provide assurance over compliance with key controls in place to ensure the Council's arrangements for the appointment of agency staff and consultants are compliant with statutory requirements and corporate policies and procedures.

This review focused on controls over policies and procedures, compliance with statutory requirements, achieving value for money and compliance with the Council's Contract Procedure Rules (CPRs). In 2022/23, the total expenditure on agency workers was £249,340 and from 1st April 2023 to 31st July 2023 spend has been £54,907.

The audit confirmed that there are documented procedures in place to determine processes for engaging agency workers and consultants. Sample testing, however, highlighted some instances of non-compliance with these procedures. There is scope for improved record keeping in some areas, which are detailed further within the audit report and action plan.

Agency worker and consultant expenditure should be undertaken in accordance with the Council's Contract Procedure Rules (CPRs). Testing performed by Internal Audit, on a sample basis, confirmed that there is scope for improvement in this area, with four of the nine cases tested evidenced as compliant with the CPRs. The Council is required to ensure that expenditure is transparent, with mechanisms that demonstrate value for money. A formal procedure is required for the approval of additional spend over the initial approved expenditure amount, which had been exceeded in 55% of cases tested.

Based on the work performed during the audit, assurance opinions were given as follows:

Assurance Opinion	
Control Environment	**Moderate** ●
Compliance	**Moderate** ●
Organisational Impact	**Medium** ●

Information governance

The primary aim of information governance is to establish compliance with statutory obligations set out in the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018). Following the introduction of the GDPR in May 2018 (amended to UK GDPR in January 2020), an internal audit took place in February 2021 to provide assurance over compliance with the GDPR and DPA in handling personal data across the Council, with overall good assurance given. In July 2022 a Rolling Risk Assurance Review was completed by Internal Audit. This was a light-touch review providing targeted testing of the data protection risk outlined within the Corporate Risk Register, providing assurance that key controls were in place and operating as expected. The review provided a 'Green' rating – representing minimal weakness that presents low risk assurance, with three recommendations agreed, these included implementing mandatory annual data protection training for all staff. This recommendation has been implemented with 100% of officers completing the training for 2023/24.

The objective of this audit was to provide assurance that controls are in place to ensure personal data is processed in accordance with the UK GDPR Principles. This review focused on controls over data sharing, data breaches/incidents, an individual's data rights and transparency.

Based on the audit testing performed, the Council appears to be compliant with the regulations in the areas within the scope of this audit. The Council has established sound information governance working practices, with guidance available to both staff and customers via the Council's intranet and website.

The use of Data Protection Impact Assessments is established, with guidance and support available to staff. A review of the Council's information rights requests (including data subject access requests) arrangements found comprehensive processes and guidance available to both staff and customers. Evidence was provided to demonstrate how data breaches/incidents are managed and investigated, with some areas for improvement to record keeping noted. Testing of the Council’s transparency obligations identified a light-touch review of the Council’s published privacy notices is required to ensure compliance with the regulations.

Based on the work performed during the audit, assurance opinions were given as follows:

Assurance Opinion		
Control Environment	**Good**	●
Compliance	**Good**	●
Organisational Impact	**Low**	●

2.4 **Implementation of audit recommendations by officers**

Where an Internal Audit review identifies any areas of weakness or non-compliance with the control environment, recommendations are made and an action plan agreed with management, with timeframes for implementation.

Since the last Committee meeting, four agreed actions have been implemented by officers. An overview is provided in Table 2.

At the time of reporting, there are six actions which remain overdue for implementation. Of these, there is one action categorised as ‘Medium’ priority which is more than three months overdue. Further details are provided in Table 3.

Table 1 - Progress against 2023/24 Internal Audit Plan

						Assurance Opinion			
Assignment		**Planned start**	**Status**		**Assurance sought**	**Control Environment**	**Compliance**	**Org impact**	**Comments**
Key financial systems									
Bank reconciliation		Q4	Not started						
Creditors		Q4	Not started						
Debtors		Q4	Not started						
Payroll		Q4	Not started						
Treasury management		Q4	Not started						
Budgetary control		Q4	Not started						
Key policy compliance									
Fees and charges		Q1	**Final report issued**		To provide assurance over the setting of fees and charges for Council services and the consistent application of these in invoicing. To cover both statutory and discretionary fees and charges.	**Moderate**	**Moderate**	**Medium**	Reported in July 2023
Payment Card Industry Data Security Standard (PCI DSS)		Q1	**Final report issued**		To review the Council's compliance with the Payment Card Industry Data Security Standard (PCI DSS) in handling of customer payments.	**Limited**	**Moderate**	**Medium**	See section 2.3
Risk based audits									
Use of agency staff and consultants		Q1	**Final report issued**		To provide assurance on procurement and management of agency staff and consultants to secure value for money and compliance with policies and IR35.	**Moderate**	**Moderate**	**Medium**	See section 2.3

						Assurance Opinion			
Assignment		**Planned start**	**Status**		**Assurance sought**	**Control Environment**	**Compliance**	**Org impact**	**Comments**
Information governance		Q2	**Final report issued**		To provide assurance over compliance with the data protection legislation and pro-active management of the associated risks in handling, storing, processing and sharing of information.	**Good**	**Good**	**Low**	See section 2.3
Community Infrastructure Levy		Q2	Draft report						
Governance of trading companies		Q2	Fieldwork underway						
Private sector housing enforcement and empty homes strategy		Q3	Not started						
Grant claims		As required	**Complete**			**Disabled facilities grant audit complete**			
IT audits									
Cyber security		Q2	Fieldwork underway						
Governance and Counter Fraud									
Counter Fraud support / promotion / policies		Q2	As required		Not applicable – consultancy work.	Daily monitoring of Report Fraud mailbox			
National Fraud Initiative		Q3	Ongoing		Not applicable – consultancy work.				Matches under review.
Risk management support and real time assurances		Q1 – Q4	Ongoing		Ongoing assurances over the controls listed in the Risk Register and supporting embedding of risk management.	Assurances provided on risk entries throughout the year.			See Table 4
Annual Governance Statement support		Q1	**Complete**						
Procurement compliance		Q4	Not started						

Table 2 - Implementation of agreed management actions

	'High' priority recommendations		'Medium' priority recommendations		'Low' priority recommendations		Total	
	Number	**% of total**	**Number**	**% of total**	**Number**	**% of total**	**Number**	**% of total**
Actions due and **implemented** since last Committee meeting	-	-	3	43%	1	33%	4	40%
Actions **overdue by less than three months**	-	-	3	43%	1	33%	4	40%
Actions **overdue by more than three months**	-	-	1	14%	1	33%	2	20%
Totals	**-**	**-**	**7**	**100%**	**3**	**100%**	**10**	**100%**

Table 3 – Actions overdue more than three months (High or Medium priority)

Audit plan	Audit title	Agreed action and context	Priority	Responsible officer	Date for implementation	Officer update / revised date
2022/23	Staff claims	**Review of Essential Car User Scheme -** To conduct a review of all 43 individuals allocated to the Essential Car User Scheme, with a particular focus on individuals that have not submitted claims this year to date. Ensure accurate allocation of individuals on to the appropriate car user scheme in line with their duties and the Council’s Remote Working Policy.	Medium	HR Manager	31/05/2023	In progress to meet a revised December 2023 deadline. This exercise needs to coincide with the new Travel and Expenses Policy.

Table 4: Customer Satisfaction

At the completion of each assignment, the Auditor issues a Customer Satisfaction Questionnaire (CSQ) to each client with whom there was a significant engagement during the assignment. There have been four survey responses received during the year to date.

Responses	N/A	Outstanding	Good	Satisfactory	Poor
Design of assignment	-	1	2	1	-
Communication during assignment	-	1	3	-	-
Quality of reporting	-	1	3	-	-
Quality of recommendations	-	1	2	1	-
Total	**-**	**4**	**10**	**2**	**-**

Glossary

At the completion of each assignment the Auditor will report on the level of assurance that can be taken from the work undertaken and the findings of that work. The table below provides an explanation of the various assurance statements that the Committee might expect to receive.

Compliance Assurances		
Level	**Control environment assurance**	**Compliance assurance**
Substantial 🟢	There is a sound system of internal control to support delivery of the objectives.	The control environment is operating as intended with no exceptions noted which pose risk to delivery of the objectives.
Good 🟢	There is generally a sound system of internal control, with some gaps which pose a low risk to delivery of the objectives.	The control environment is generally operating as intended with some exceptions which pose a low risk to delivery of the objectives.
Moderate 🟡	There are gaps in the internal control framework which pose a medium risk to delivery of the objectives.	Controls are not consistently operating as intended, which poses a medium risk to the delivery of the objectives.
Limited 🔴	There are gaps in the internal control framework which pose a high risk to delivery of the objectives.	Key controls are not consistently operating as intended, which poses a high risk to the delivery of the objectives.
No 🔴	Internal Audit is unable to provide any assurance that a suitable internal control framework has been designed.	Internal Audit is unable to provide any assurance that controls have been effectively applied in practice.

Organisational Impact	
Level	**Definition**
High 🔴	The weaknesses identified during the review have left the Council open to a high level of risk. If the risk materialises it would have a high impact upon the organisation as a whole.
Medium 🟡	The weaknesses identified during the review have left the Council open to medium risk. If the risk materialises it would have a medium impact upon the organisation as a whole.
Low 🟢	The weaknesses identified during the review have left the Council open to low risk. This may have a low impact on the organisation as a whole.

Limitations and Responsibilities

Limitations inherent to the internal auditor's work

Internal Audit is undertaking a programme of work agreed by the Council's senior managers and approved by the Audit Committee subject to the limitations outlined below.

Opinion

Each audit assignment undertaken addresses the control objectives agreed with the relevant, responsible managers.

There might be weaknesses in the system of internal control that Internal Audit are not aware of because they did not form part of the programme of work; were excluded from the scope of individual internal assignments; or were not brought to Internal Audit's attention.

Internal control

Internal control systems identified during audit assignments, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and unforeseeable circumstances.

Future periods

The assessment of each audit area is relevant to the time that the audit was completed in. In other words, it is a snapshot of the control environment at that time. This evaluation of effectiveness may not be relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulatory requirements or other factors; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management; internal control and governance; and for the prevention or detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

Internal Audit endeavours to plan its work so that there is a reasonable expectation that significant control weaknesses will be detected. If weaknesses are detected additional work is undertaken to identify any consequent fraud or irregularities. However, Internal Audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected, and its work should not be relied upon to disclose all fraud or other irregularities that might exist.